FORTINET
High Performance Network Security

FortiWLC

Release 8.3.2
(Virtual Controllers)

FortiWLC-SD 8.3.2 is a **limited release delivering the new Virtual Controllers**. Additionally, this release also introduces features and enhancements as listed under New Features section.

To ensure a secured WiFi network, Fortinet controllers and access points are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware.

Fortinet Wireless LAN Virtual Controllers

With this release of FortiWLC-SD, the FWC-VM Series Virtual Controllers - **FWC-VM-50, FWC-VM-200, FWC-VM-500, FWC-VM-1000**, and **FWC-VM-3000** are introduced.

For more information on deploying the Virtual controllers, see the *Virtual Controller Deployment Guide*.

Supported Hardware Configuration

The following table displays the minimum supported configuration for each of the virtual controller models.

Virtual Controller Model	Number of CPUs	RAM (GB)
FWC-VM-50	4	4
FWC-VM-200	4	8
FWC-VM-500	8	16
FWC-VM-1000	24	32
FWC-VM-3000	48	64

Supported Virtual Platforms

With this release of FortiWLC-SD, the supported virtual platforms are VMware, Linux KVM, and Windows Hyper-V.

Supported Hardware and Software

Hardware and	Supported		Unsupported
Access Points	AP122 AP822e, AP822i (v1 & v2) AP832e, AP832i, OAP832e AP332e, AP332i* AP433e, AP433i, OAP433e* FAP U421EV FAP U423EV	AP1010e, AP1010i* AP1020e, AP1020i* AP1014i* AP110	AP201 AP208 AP150 AP300, AP301, AP302, AP302i, AP301i AP310, AP311, AP320, AP310i, AP320i OAP180
*Cannot be configured as a relay AP			
Controllers	FWC- VM-50# FWC –VM-200# FWC –VM-500# FWC –VM-1000# FWC-VM-3000#	#Spectrum Manager NOT supported in these controller models	
FortiWLM	8.3.2		
FortiConnect	16.8		
Browsers			
FortiWLC (SD) WebUI	Internet Explorer 9,10 Mozilla Firefox 25+ Google Chrome 31+		
A limitation of Firefox 3.0 and 3.5+ prevents the display of the X-axis legend of dashboard graphs.			
Captive Portal	Internet Explorer 6, 7, 8, 9, 10, IE11 and Edge. Apple Safari Google Chrome Mozilla Firefox 4.x and earlier Mobile devices (such as Apple iPhone and BlackBerry)		

Installing 8.3.2 on Virtual Controllers

Obtain a signed image file for the appropriate hypervisor module and install accordingly.
A freshly installed system boots up as FWC-VM-50 with a default license valid for 30 days. After VM image installation, with all necessary resources allocated, VM is capable of emulating any virtual platform based on the product specific license.

No two Ethernet ports of virtual Controller should be connected to the same vSwitch since the port group in vSwitch is configured to be in promiscuous mode and hence both the ports will receive packets coming from all other ports in that vSwitch *including* the other port which is connected to the Controller.

For FWC-VM-3000, always connect all the ports to the VM switch. All the ports should be connected to different vSwitches whose uplinks should be connected to different ports on the external switch and all those ports should be link aggregated.

See License Management for Virtual Controllers section for importing licenses.

Upgrade Advisories

The following are upgrade advisories to consider before you begin upgrading your network.

Devices with Intel Chipset

Wireless devices with Intel chipset must upgrade its firmware to version 19.x.x.

Mesh Deployments

When attempting to upgrade a mesh deployment, you must start upgrading the mesh APs individually, starting with the outermost APs and working inwards towards the gateway APs before upgrading the controller.

Feature Groups in Mesh profile

If APs that are part of a mesh profile are to be added to feature group, all APs of that mesh profile should be added to the same feature group. The Override Group Settings option in the ***Wireless Interface*** section in the Configuration > Wireless > Radio page must be enabled on the gateway AP.

Captive Portal and Fortinet Connect Deployment Recommendations

DNS Entry

It is mandatory to enter the DNS while creating internal DHCP profile.

External Portal IP Configuration

If a NAT device is located between the controller and the Fortinet Connect, the IP address with which Fortinet Connect sees the controller should be configured under Device > RADIUS Clients page in Fortinet Connect Admin portal (*http://<fortinetconnect-ip-address>/admin*), . Select the RADIUS client and enter the controller IP address in the Client tab. The Fortinet Connect Automatic Setup then configures the controller correctly and ensures that the correct controller IP address is configured on Fortinet Connect.

Remember Me settings

In the Portal Settings step of the Guest Portal configuration wizard, if you choose to enable Remember Credentials, then select "Initially attempt to use a cookie, if this fails try the MAC address" option. This removes the dependency on the client's browser and security settings.

SmartConnect Certificate download

In the Certificates step of the Smart Connect Profile Wizard, ensure that you select the complete certificate chain of your uploaded certificate. If all certificates in the chain (from root to server) have been uploaded, then selecting the server certificate will automatically select the entire certificate chain.

- To upload the server certificates, go to **Server > SSL Settings > Server Certificate** tab.
- To upload rest of the chain, go to **Server > SSL Settings > Trusted CA Certificates** tab

CNA Bypass for Android 5.0 +

Devices running Android 5.0 and above introduces system default CP login pop-up windows. To disable this pop-up window enable CNA bypass in the controller.

In the WebUI

Go to **Configuration > Security > Captive Portal** > Advanced Settings section, select Captive Portal Profile and set **Apple Captive Network Assistant** (CNA) Bypass to ON.

Using CLI

Use the **`ssl-server cna-bypass`** ON command in config mode.

Voice Scale Recommendations

The following voice scale settings are recommended if your deployment requires more than 3 concurrent calls to be handled per AP. The voice scale settings are enabled for an operating channel (per radio). When enabled, all APs or SSIDs operating in that channel enhances voice call service. To enable:

1. In the WebUI, go to **Configuration > Devices > System Settings > Scale Settings** tab.
2. Enter a channel number in the *Voice Scale Channel List* field and click **OK**.

Enable the voice scale settings only if the channel is meant for voice deployment.
After enabling voice scale, the voice calls in that channel take priority over data traffic and this result in a noticeable reduction of throughput in data traffic

IP Prefix Validation

In a situation where a station with an IP address from a different subnet connects to the controller, it can result in various network issues including outage. A new field, IP Prefix Validation is added to the ***ESS Profile*** and ***Port Profile*** configuration page. When enabled, stations with different subnet are prevented from connecting to the controller. By default, IP Prefix Validation in **ESS Profile is ON** and in **Port Profile it is OFF**.

IP Prefix Validation must be disabled if the ESS profile is used for RAC.

QoS Rules

QoS rules with no matching criteria when Match is checked will abort an upgrade. To prevent this, check QoS rules to ensure that at least one matching criteria is set for each rule if Match is set.

New Features

- Virtual Controllers
- Support for Beacon Services
- Spectrum Analysis Support on FAP
- 802.3af support for FAP42x
- 256 clients support for FAP
- Hotspot 2.0 Enhancements
- Change of Authorization (CoA) Enhancements

Virtual Controllers

This release introduces the new FWC-VM Series Virtual Controllers with the following models:

- FWC-VM-50
- FWC-VM-200
- FWC-VM-500
- FWC-VM-1000
- FWC-VM-3000

The Fortinet Virtual Controllers can now be deployed on the Linux KVM and Windows Hyper-V platforms.

For more information on deploying the Fortinet Virtual Controllers, see the *Virtual Controller Deployment Guide*.

License Management

After completing installation of the Virtual Controller, login to the controller and run the **setup** command to generate the system-id. Perform the following steps to obtain the license.

1. Run the **setup** command on the Controller to generate the system-id, configure the hostname, and configure the static IP address of the Controller, to ensure that the IP address does not change as the system-id/license is mapped to the IP address of the Controller.
2. Save the configuration. The Controller restarts.
3. Run the **show system-id** command to obtain the system-id.
4. Share the Virtual Controller model details, system-id, and the license validity period (or permanent license) with the Forticare Support team.
5. Configure the Virtual Controller instance with the required resources as per the model for which the license has been generated.
6. Install the license from the GUI (See section *Importing and installing a License*) OR from the CLI (Configuration Terminal mode => **vm-license scp://username@<Your file server IP Address>:<license filename>**)
7. Restart the Controller to apply the changes as per the generated license.

Note: A freshly installed system boots up as FortiWLC-50D-VM with default license valid for 30 days.

- System-id is not get generated until you run the **setup** command on a fresh instance.
- System-id is coupled with the IP address. Hence, any change in the IP address generates a new system-id thereby failing validation of the older license. In this case,

a new license is required. Changing the IP address via CLI followed by a reboot to activate the new IP address does not generate a new system-id. Hence, license validation fails and the controller is once again the FortiWLC-50D-VM model. Therefore, use only the **Setup** command to change the Controller IP address.

Importing and Installing a License

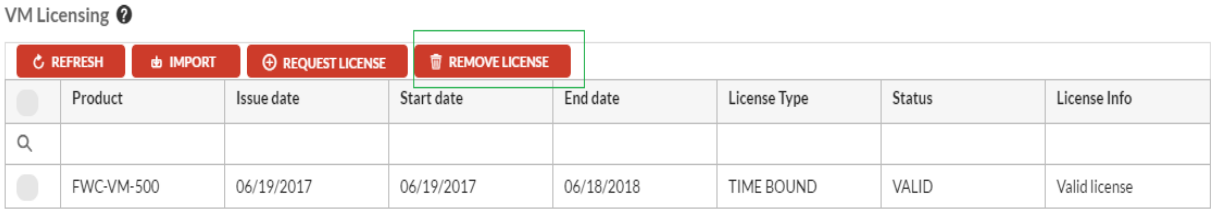
Perform these steps to obtain the license using the GUI.

1. Navigate to **Maintenance > System > VM Licensing**
   This image displays a freshly installed system which has a default license (trial based) valid for 30 days from the license issued date.
2. In the **VM Licensing** wizard, click **Import** to add a license. By default, this page lists the license available on the system which includes details on the Virtual Controller model.

License Validation

After the license is imported, validation is performed on the license parameters. If that validation succeeds and the appropriate hardware resources for the requested controller model are allocated, then the license is installed successfully. If either license validation or hardware resource validation fails, the system reverts to the default license. See section *Supported Hardware Configuration* for further details.

Once the license is installed successfully, it replaces the default license. There are two types of licenses – Time Bound and Perpetual (Never ending).



License Monitoring

The license validation happens after every one hour at regular intervals. With 30 days to go for expiry, alarms are raised on the controller. The Software License Expired alarm is generated as per the configured severity. The default severity is critical.

In a fresh installation running on a default license (FWC-VM-50) which is valid for 30 days, you get 30 additional days within which to purchase and apply for a valid license. If a valid license is not imported, at the end of additional 30 days, the Controller will reboot and the APs will go to offline state.

For a system already running on a valid license, the user has 30 additional days following the expiry of the license to renew the license. If the license is not renewed, at the end of additional 30 days, the Controller will reboot and the APs will go to offline state.

Support for Beacon Services

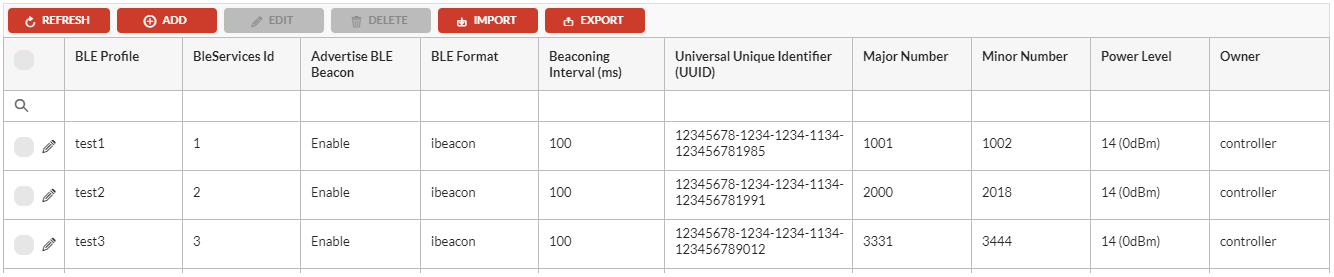
With this release of FortiWLC-SD, support for beacon services has been enhanced. You can now create multiple Beacon Service profiles and also map APs to a specific profile. The APs part of a profile send iBeacons that help advertise hyperlocal content to users in the context of their location.

The BLE services are available by default in FAP U421EV and FAP U423EV. For other non-wave2 APs, you need Bluetooth adapters, for example, Broadcom USB Class 2 Bluetooth 4.0 Dongle, CSR 4.0 Bluetooth Dongle and Iogear Bluetooth 4.0 USB Micro Adapter GBU521). Ensure that Bluetooth adapters support Bluetooth version 4.0 or above.

Note: Access points must be connected to 802.3at power supply.

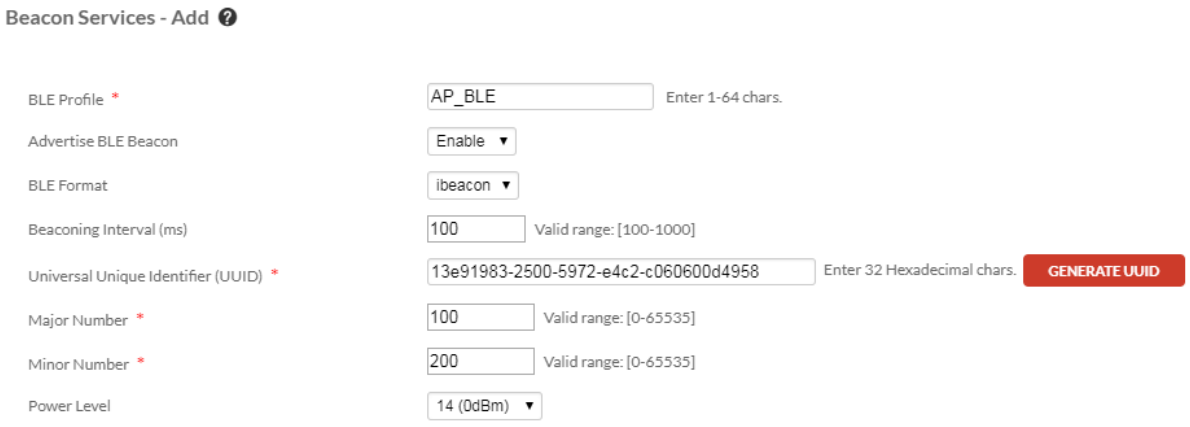
Creating a Beacon Service Profile

1. Navigate to **Configuration > Devices > Beacon Services.**



BLE Profile	BleServices Id	Advertise BLE Beacon	BLE Format	Beaconing Interval (ms)	Universal Unique Identifier (UUID)	Major Number	Minor Number	Power Level	Owner
test1	1	Enable	ibeacon	100	12345678-1234-1234-1134-123456781985	1001	1002	14 (0dBm)	controller
test2	2	Enable	ibeacon	100	12345678-1234-1234-1134-123456781991	2000	2018	14 (0dBm)	controller
test3	3	Enable	ibeacon	100	12345678-1234-1234-1134-123456789012	3331	3444	14 (0dBm)	controller

2. In the Beacon Services, click the **ADD** button and enter the following:



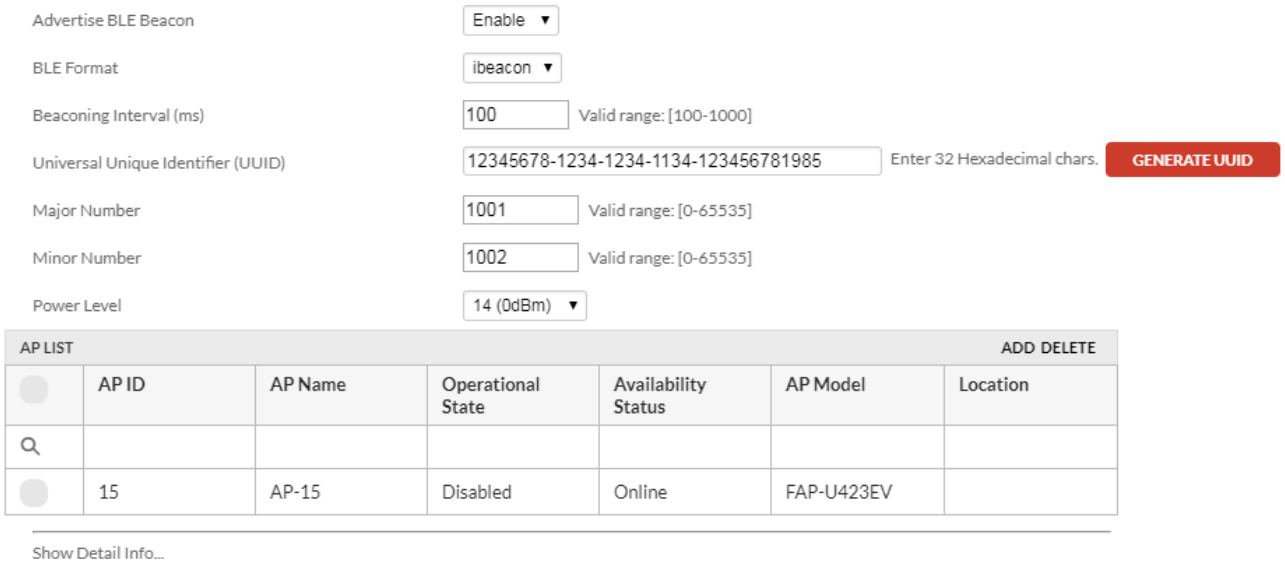
- **Ble Profile** – Name for this BLE Profile.
- **Advertise BLE Beacon** – Enable/Disable beacon services.
- **BLE Format** – Select ibeacon as a BLE Format.
- **Beacon Interval** – Select the time interval at which the Beacons are to be sent.
- **Universal Unique Identifier (UUID**) – Enter a UUID that is specific to the network.
- **Major Number** – Select a Major Number.

- **Minor Number** – Select a Minor Number.
- **Power Level** – Select a Power Level.

Note: A maximum of 3000 Beacon service profiles can be created

Adding APs to the Beacon Service Profile

Click the edit icon to view the service profile details. **Beacon Services – Update** page is displayed to make changes to the service profile.

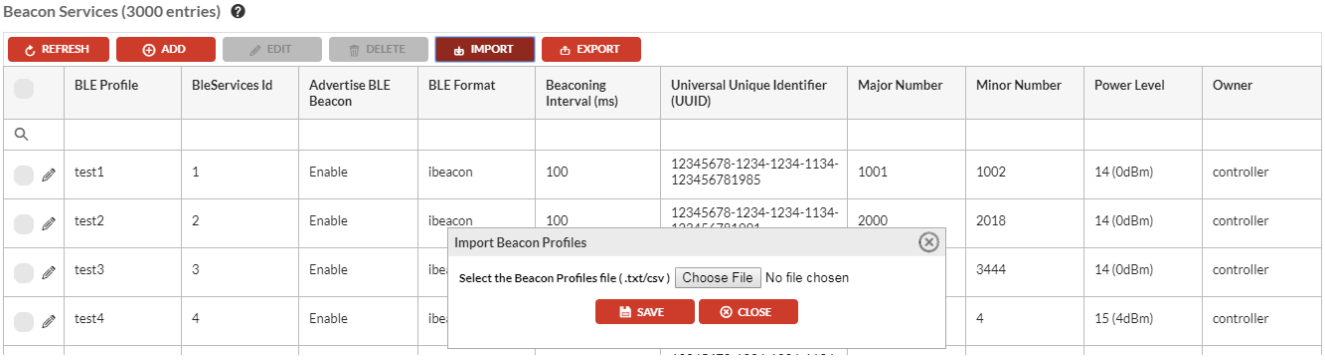


Click the **Add** option to start adding APs to the service profile. By default this page shows the list of APs added to the service profile.

- You can add multiple APs to a service profile
- An AP can be mapped to only one service profile at a time

Importing and Exporting Beacon Service Profiles

Users can import/export the Beacon Service Profiles through the CLI and GUI. The supported file formats are .txt and .csv



Spectrum Analysis Support on FAP

With this release of FortiWLC-SD, spectrum analysis support for FAP U421EV and FAP 423EVaccess points with Advanced Interference detection mechanism has been added.

You can deploy these APs in your wireless network scans the environment continuously for interference and sends reports to Spectrum Manager on the interference detected.

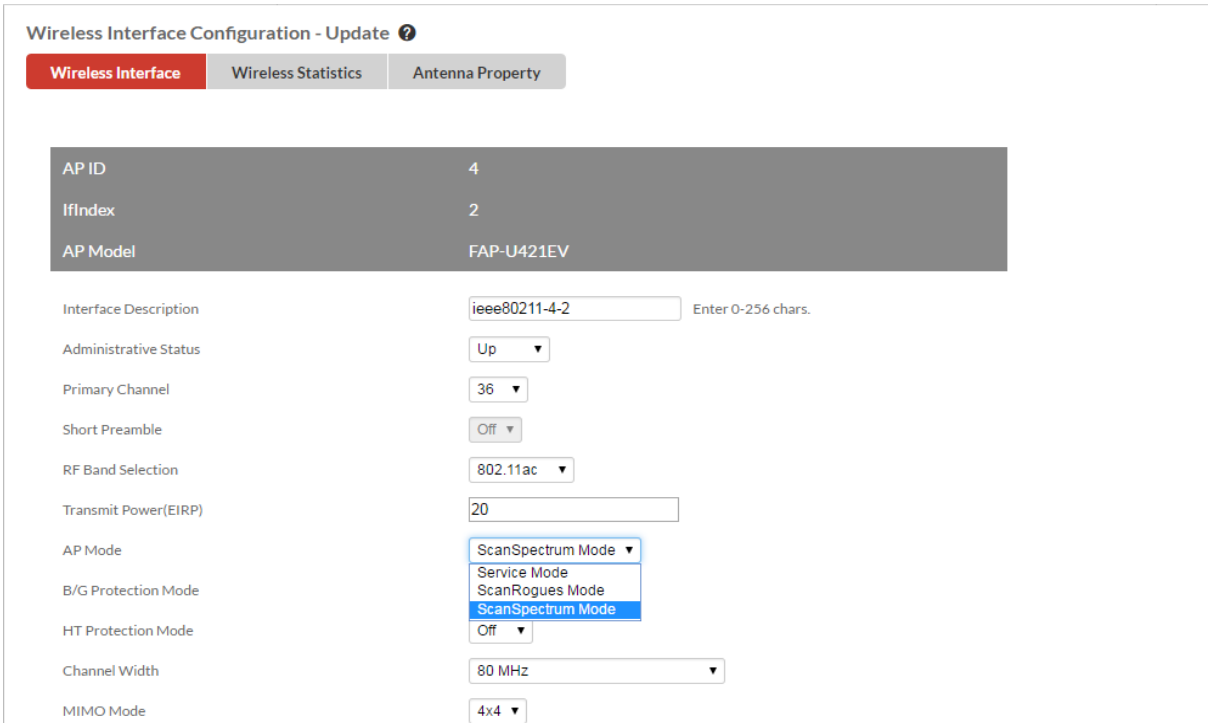
Note: The APs need to be discovered in L3 mode for the scan spectrum functionality to work

Interference from the following devices can be detected with the help of spectrum analysis:

- Microwave Oven (conventional)
- Analog Cordless Phone (2.4 and 5 GHz)
- Wireless video camera (2.4 and 5 GHz)
- Wideband RF Jammer
- Narrowband RF Jammer
- S-Band radar-based motion detector
- DSSS Cordless Phone (2.4 and 5 GHz)
- Digital Baby Monitor – Single Carrier
- Microwave Oven (inverter)
- Xbox wireless game controller
- Bluetooth Device
- FHSS Cordless Phone (2.4 and 5 GHz)
- Possible Interferer

Enabling Spectrum Analysis

1. Navigate to **Configuration > Wireless > Radios**.
2. Click the edit icon on the radio for the AP which needs to be enabled to scan the spectrum.

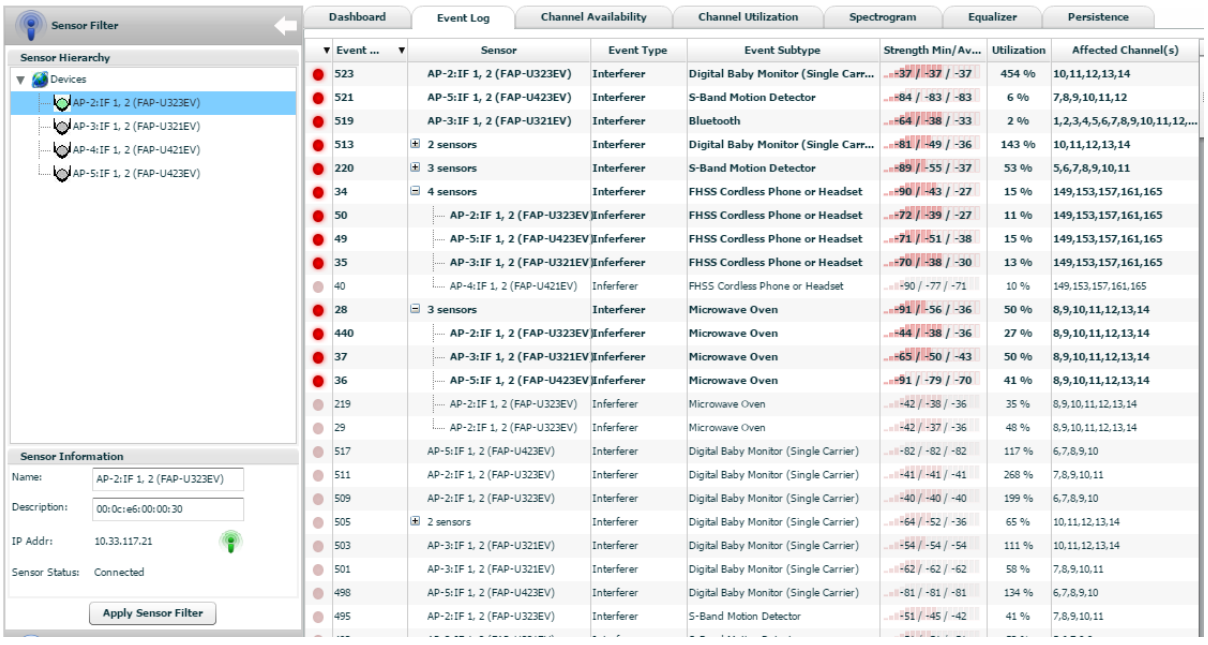


3. Change the AP mode from **Service Mode** to **ScanSpectrum Mode.**

Note: The AP will not service clients in **ScanSpectrum Mode**.

Once Scan Spectrum is enabled for a particular radio of an AP, the sensor in that AP starts scanning and reports events to the Spectrum Manager. Each radio interface of the AP scans only the corresponding band (2.4GHz or 5GHz) it is configured for.

Events on spectrum analysis cannot be viewed on the new VM controllers.



802.3af Support for FAP42x

With this release of FortiWLC-SD, support for FAP U421EV, FAP U423EV access points powering up when connected to 802.3af PoE source is provided.

- FAPs powered using 802.3af power, will boot up and operate in 2x2 MIMO mode with 17dbm transmit power. The USB port will be disabled on these FAPs.
- FAPs powered using 802.3at, will continue to operate in the configured mode with default transmit power.

256 Clients Support for FAP

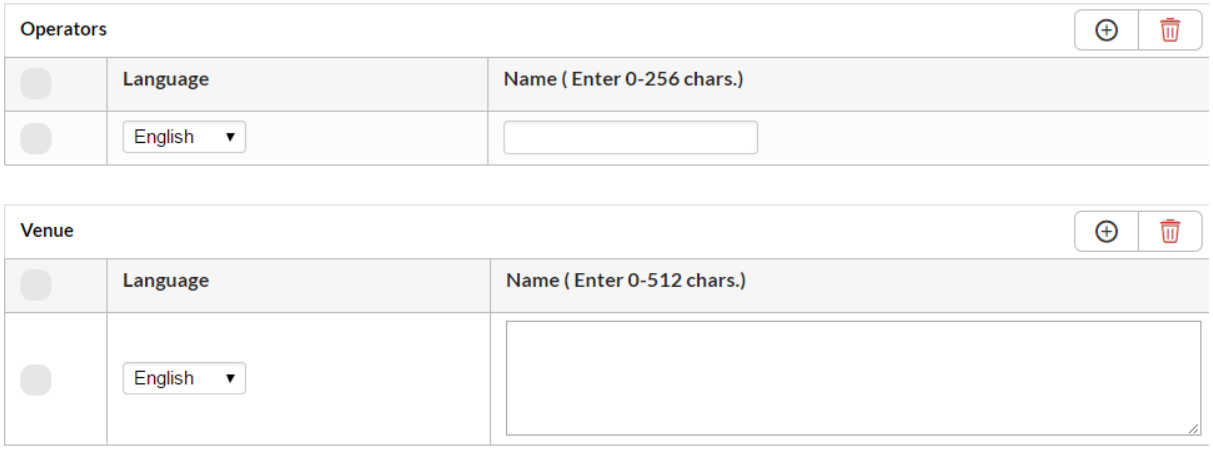
With this release of FortiWLC-SD, FAP U421EV and FAP U423EV access points can support up to 256 clients per radio interface. The 256 client support per radio is only for a native cell environment. In a virtual cell environment, the maximum clients supported per interface are 170.

Hotspot 2.0 Enhancements

With this release of FortiWLC-SD, additional configuration parameters are included when creating a hotspot profile from **Configuration > Wireless > Hotspot 2.0.**

Add Hotspot Profile

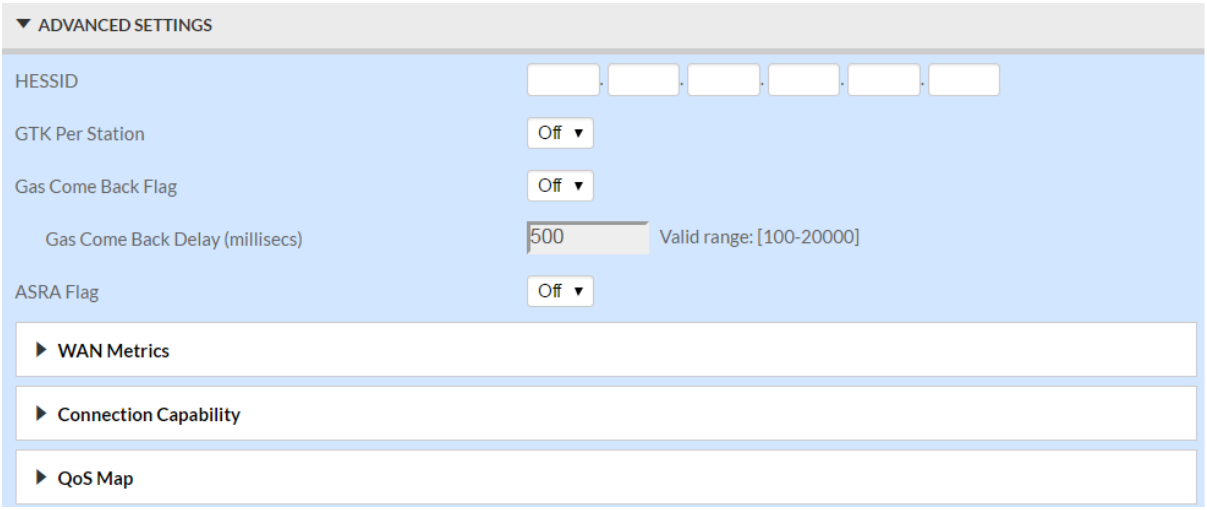
1. Select **Configuration > Wireless > Hotspot.**
2. Click **Add.**



The additional parameters available with this release are:

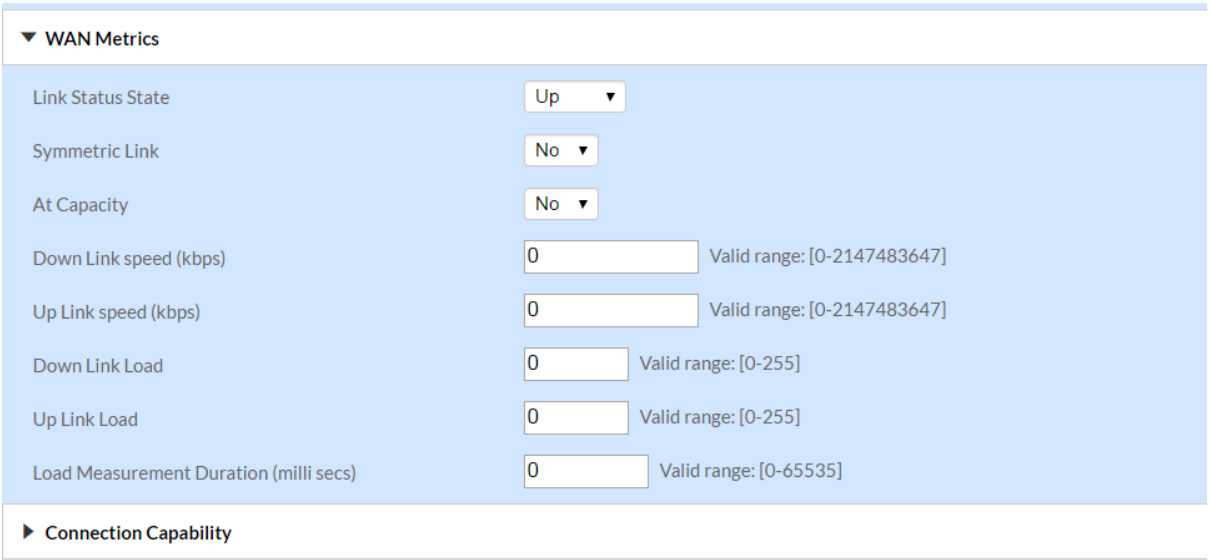
- Options to add multiple operator names
  - Select Language from the drop down menu
  - Enter Operator Name (0-256 characters)
- Option to add multiple Venues
  - Select Language from the drop down menu
  - Enter Venue Name (0-512 characters)

Advanced Settings



- **HESSID** – APs homogeneous ESS ID.
- **GTK per Station** – Select On/Off.
- **Gas Come Back Flag** – Select On/Off.
- **Gas Come Back Delay** – If ON, set delay in milliseconds. Valid range is 100-20000.
- **ASRA Flag** – Select On/Off. If **ASRA Flag** is set to ON, enter the following:
- **Authentication type** – Enter the Authentication type.
- **Redirect URL** – Enter the redirection URL.

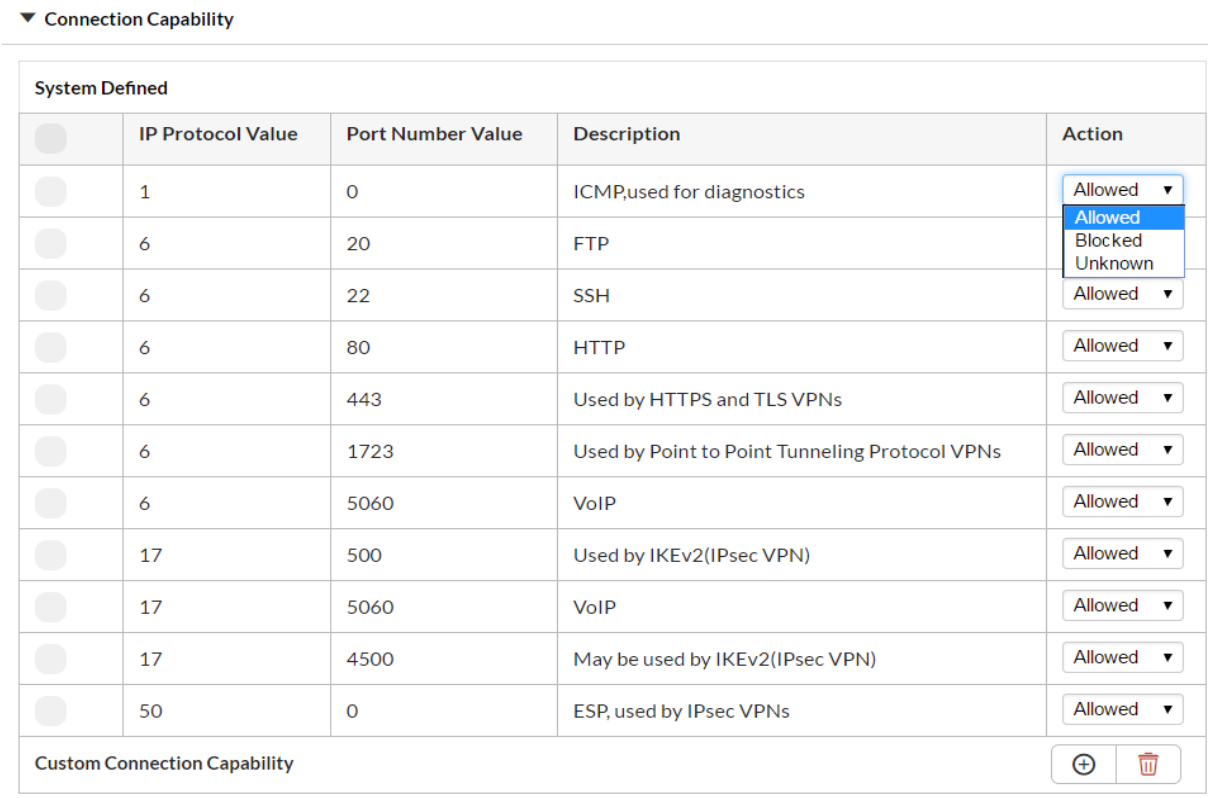
WAN Metrics



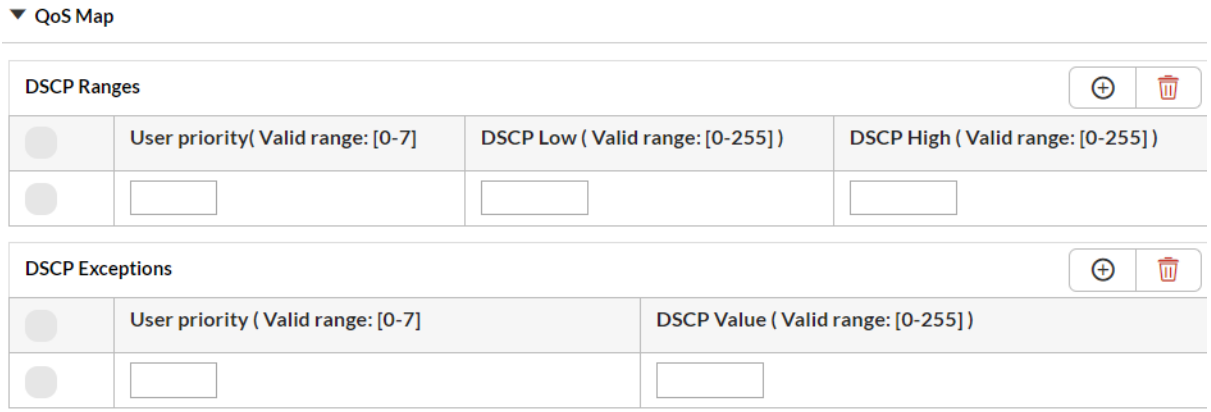
- **Link Status State** – Can be set to Up/Down/Testing.
- **Symmetric Link** – Select Yes/No. Default setting is No.
- **At Capacity** – Select Yes/No. Default setting is No.
- **Downlink Speed** – Enter downlink speed in kbps. Valid range is 0-255.
- **Uplink Speed** – Enter uplink speed in kbps. Valid range is 0-255.
- **Load Measurement Duration** – Enter duration in milliseconds. Valid range is 0-65535.

Connection Capability

The connection capabilities allow you to allow/block protocols. There is a set of system defined protocols. In addition, you can also create rules for custom protocols.



QoS Map



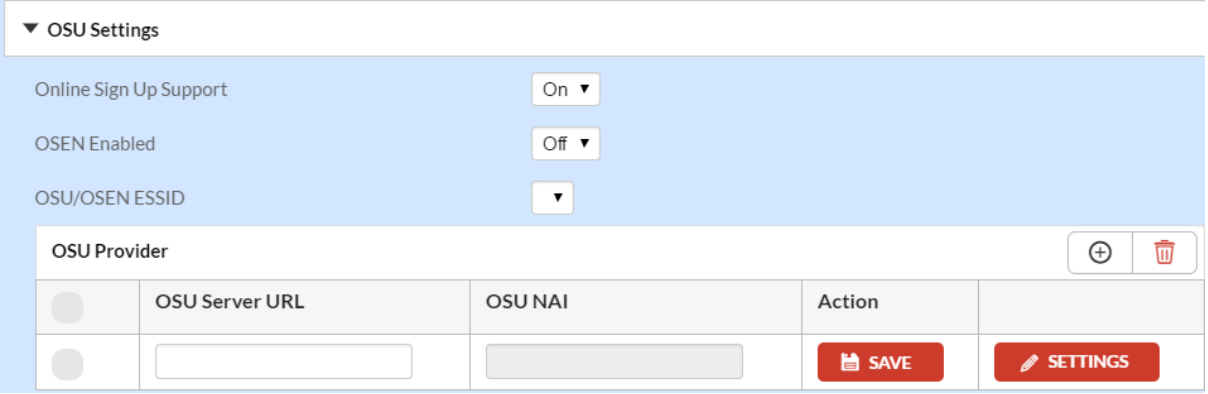
Option to set DSCP ranges.

- Set User Priority. Valid range is 0-7
- Set DSCP Low. Valid range is 0-255
- Set DSCP High. Valid range is 0-255

Option to set DSCP Exceptions.

- Set User priority. Valid range is 0-7
- Set DSCP Value. Valid range is 0-255

Once the profile is created, additional parameters are available under **Advanced Settings**.



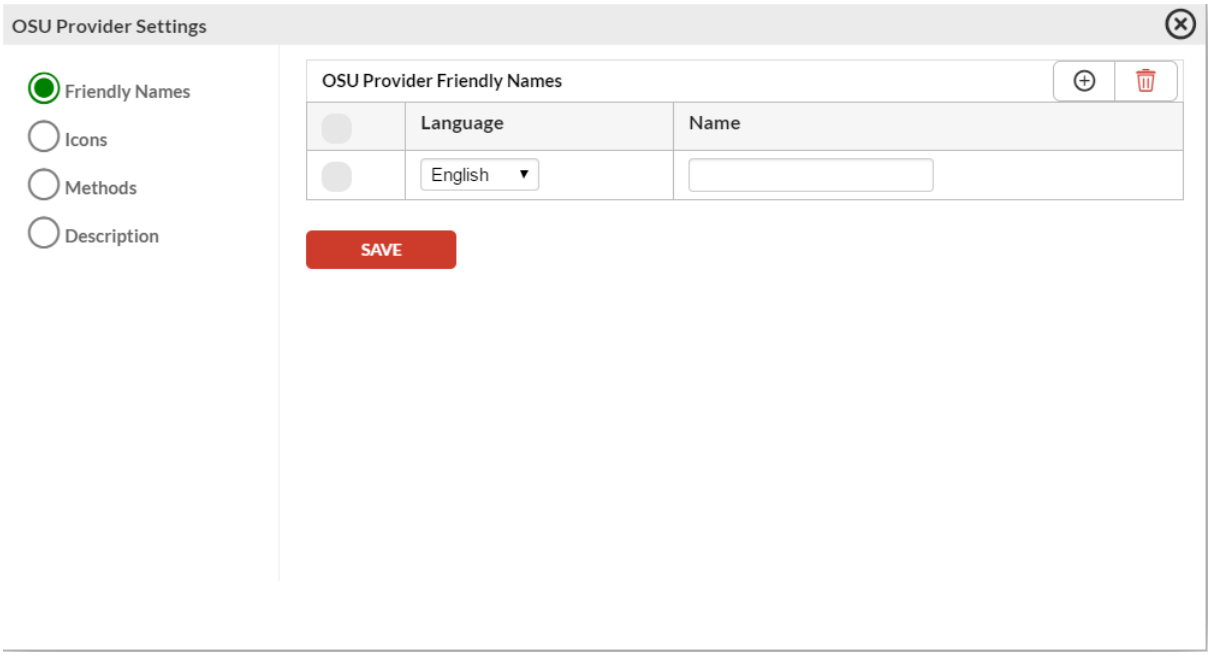
Online Sign Up Support – Select On/Off. When set to On, configure the following:

- OSEN Enabled – Select On/Off.
- OSU/OSEN ESSID – The OSU ESSID.

Enter the OSU Provider details.

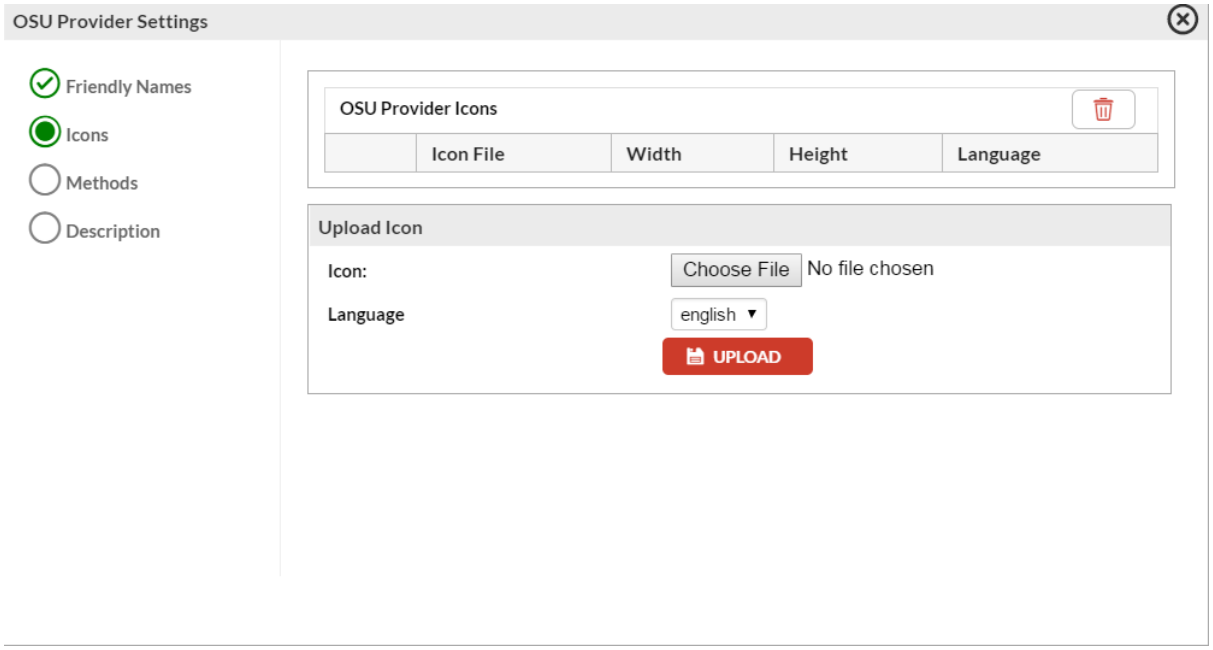
- Set OSU Server URL
- Set OSU NAI if OSEN Enabled is set to On

Click **Settings**



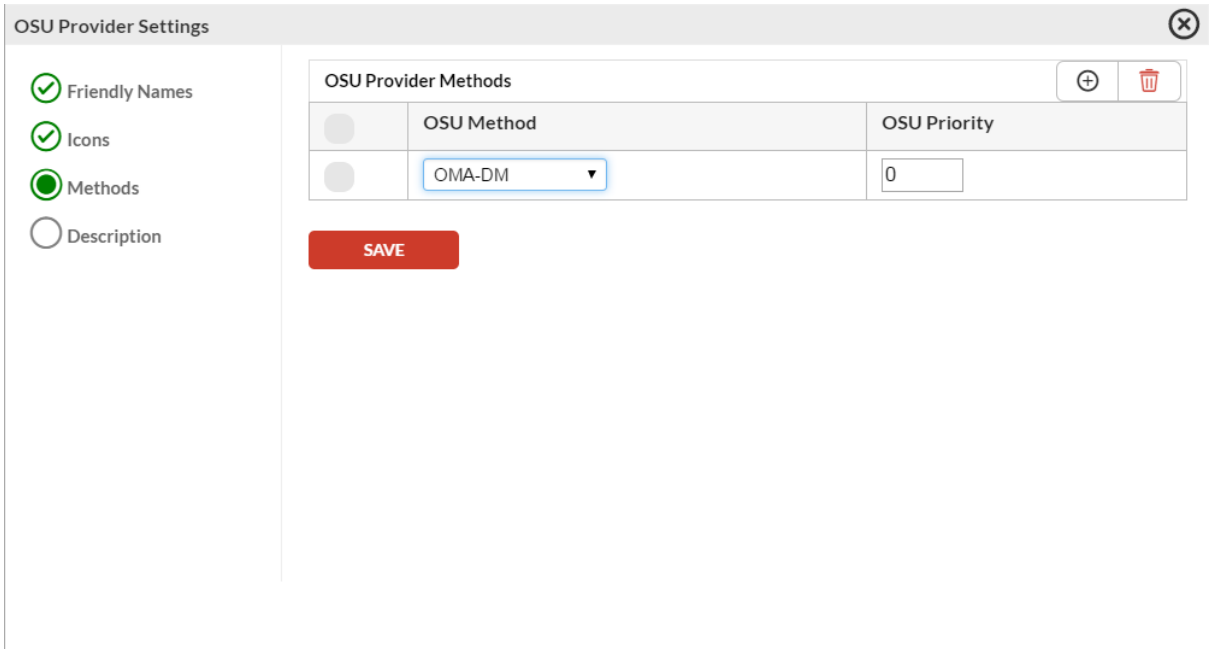
Configure the **OSU Provider Friendly Names**.

- Set Language
- Enter Name



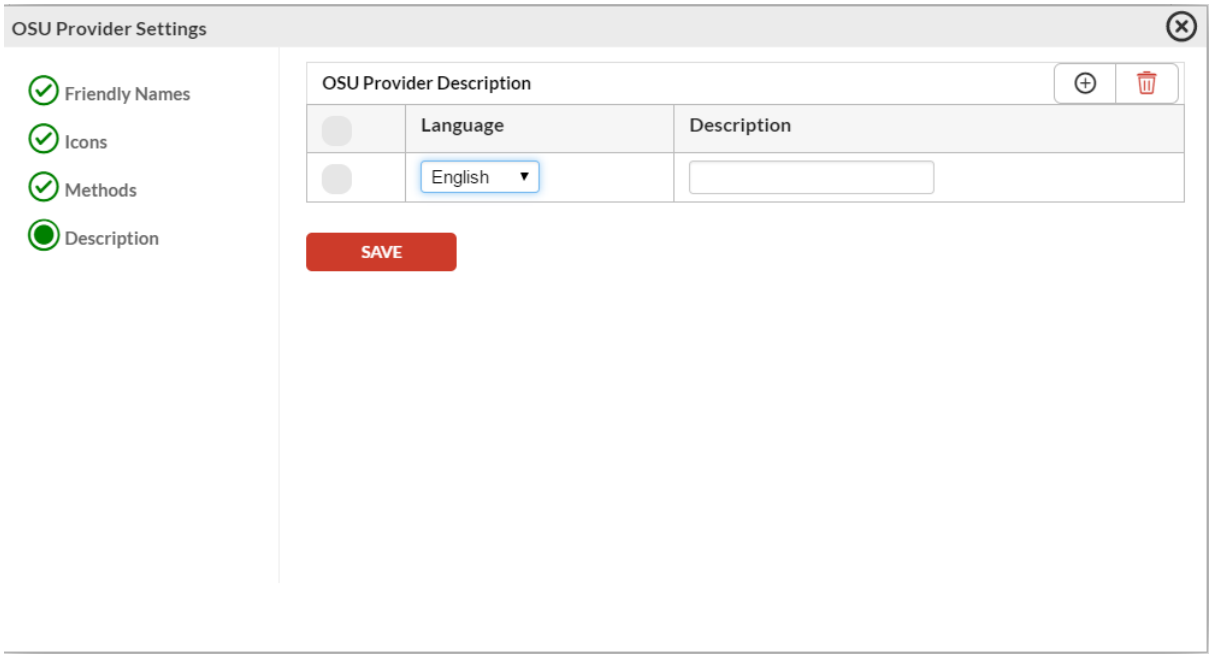
Configure the **OSU Provider Icons**.

- Select the Icon file.
- Select the Language.
- Click **Upload** to import the file.



Configure **OSU Provider Methods.**

- Select the **OSU Method** from the drop down**.**
- Select the **OSU Priority.**



Configure the **OSU Provider Description**.

- Select the **Language.**
- Enter the **Description.**

Change of Authorization (CoA) Enhancements

With this release of FortiWLC-SD, the following CoA enhancements have been made,

- Support for RADIUS based filter-ID and CoA for filter-ID change for MAC authenticated (RADIUS) clients is added (Mantis ID – 00377679)
- Changes to honour CoA disconnection requests when a user maps a security profile which is configured for WPA-PSK with MAC filtering enabled, to an ESS profile is implemented (Mantis ID – 0377253)
- CoA disconnect requests for Captive Portal (CP) Bypass and MAC filtering enabled stations will have the stations go through the complete MAC and CP authentication while re-connecting (Mantis ID – 0406337)

Fixed Issues

Bug ID	Description
415130	FortiWLC is no longer vulnerable to CVE-2017-7335. For more information, visit https://fortiguard.com/psirt.
416877	FortiWLC is no longer vulnerable to CVE-2017-7341. For more information, visit https://fortiguard.com/psirt.

Known Issues and Limitations

Bug ID	Description
433793	Mismatch in station count between the **show station** CLI command output and the GUI Dashboard in the Scale setup.
412831	The default QoS rules are not present in a fresh installation of Virtual Controllers resulting in failed SIP phones calls. **Workaround**: Run the run create_rules.cli command in Privilege-exec mode to create QoS rules.
436554	Degraded IPv4 performance with singe 10GB port when FWC-VM-500 is deployed on VMWare ESXi.
436986	Degraded IPv4 performance with singe 10GB port when FWC-VM-1000 and FWC-VM-3000 are deployed on VMWare ESXi.
416989	Degraded IPv4 performance with singe 10GB port when FWC-VM-3000 is deployed on Linux KVM.
434065	Degraded IPv4-LAG performance when FWC-VM-3000 is deployed on VMWare.
422724	Two Ethernet ports on a Virtual Controller CANNOT be connected to the same vSwitch. The port group in a vSwitch is configured to be in the promiscuous mode and hence both the ports will receive packets coming from all other ports in that vSwitch, including the other port it is connected to.
415004	VM-FWC-3000D specific: The VMware server decides (randomly) the sequence of enumeration of PCI network device ports. Hence, all the ports should be connected to different vSwitches, whose uplinks should be connected to different ports on the external switch and all those ports should be link aggregated.
435521	For License validation, the eth0 interface should always be up. Due to this limitation Dual Ethernet Redundancy does not work in Virtual Controllers.
424537	Hypervisor limitation - The speed of a 1G port connected to a network interface is always displayed as 10G.
415007	Software License Violation alarm severity will always follow the Controller global configuration of alarms severity irrespective of the remaining validity duration.

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service

change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable